

ON (MULTI)-COLLISION TIMES

ERNST SCHULTE-GEERS

ABSTRACT. We study the (random) waiting time for the appearance of the first (multi-)collision in a drawing process in detail. The results have direct implications for the assessment of generic (multi-)collision search in cryptographic hash functions.

1. INTRODUCTION

A (n, m) -function is a function $h : \mathcal{D} \rightarrow \mathcal{R}$ where $|\mathcal{D}| = n$ and $|\mathcal{R}| = m$ are finite sets.

An r -fold multi-collision (short: r -collision) of h is an r -element set $\{d_1, \dots, d_r\}$ of (mutually distinct) domain points s.th. $h(d_1) = h(d_2) = \dots = h(d_r)$, 2-collisions are called collisions.

In particular, for cryptographic hash functions h the difficulty of statistical (multi-) collision search for h is of interest : how difficult is it to find a point $y \in \mathcal{R}$ and two (resp. r) different h -preimages of y ?

In a generic statistical (multi-) collision attack on a hash function h an attacker produces randomly hash values (i.e. he produces randomly preimages of h and maps them through h) until he has found the first (multi-) collision.

How many hash values must be produced to find a (multi-)collision?

This number is a random variable - the waiting time K_r (resp. R_r) for the first (multi-) collision (resp. repetition) - and the distribution of this “collision time” describes statistically the effort needed for the (multi-)collision search.

The main questions of interest are

- (1) what is the average effort for the attack (the expectation of the collision time)?
- (2) what is the typical effort for the attack (the distribution of the collision time)?

Cryptologic “folklore” states that this question reduces to the classical birthday phenomenon in the codomain, and that the “birthday effort”- i.e. the trial of magnitude \sqrt{m} (resp. $m^{(r-1)/r}$ preimages) - is needed to find a (multi-)collision.

The folklore result relies on the underlying assumption that the mapping h behaves as a (uniform) random mapping (the individual domain points “pick” their image uniformly at random, independently of the other domain points).

It is clear - but frequently not explicitly stated - that this is an approximation.

This “random mapping” approximation was (for the collision case) questioned by Bellare and Kohno ([2]), who pointed out that the behaviour of a fixed hash

Date: February 25, 2014.

Key words and phrases. collisions, repetitions, birthday problem, generic collision attacks.

function could possibly deviate strongly from random. Their standpoint: for a given hash function one should try to quantify resistance to generic collision attacks using a balance measure (rather than to assume random mapping behaviour a priori). Similar balance measures for multi-collisions were proposed and investigated by Ramanna and Sarkar in [23]. These papers also provide “rough” statistical answers to 1. and 2. However, despite of the interest in generic attacks there is apparently a lack of rigorous results so far.

The object of this paper is to close this gap. We prove precise statistical assertions to questions (1) and (2) and give a survey of exact results on the subject.

In the sequel we consider both commonly used models for the mapping h :

(a) the mapping h is fixed (b) the mapping h is chosen at random.

Further we treat both, sampling with replacement and sampling without replacement.

2. PREVIOUS AND RELATED WORK

Statistical collision search may be thought of as a generalised “birthday problem”. (The exact relationship to the classical birthday problem is explained in §4.1 below.)

2.1. The classical birthday problem. Let $r \geq 2$. The classical r -fold birthday problem deals with the following question:

k balls are distributed at random into m cells. How big is the chance that no cell contains more than $r - 1$ balls?

The classical answer, due to von Mises [28], is as follows:

For $j \in \{0, \dots, k\}$ let $U_j^{k,m}$ be the random variable “number of cells containing exactly j balls”.

Then the following theorem holds:

Theorem 2.1. (von Mises)

Let $j \in \{0, \dots, k\}$ be fixed and $\alpha = \frac{k}{m}$. Then

$$(a) \mathbf{E}(U_j^{k,m}) = m \binom{k}{j} \left(\frac{1}{m}\right)^j \left(1 - \frac{1}{m}\right)^{k-j},$$

(b) If $k, m \rightarrow \infty$ s.th. $m^{\frac{\alpha^j}{j!}} e^{-\alpha}$ tends to a finite positive limit a_j , then asymptotically $U_j^{k,m}$ is Poisson distributed with parameter a_j .

The random variable $S_r^{k,m} := \sum_{i=r}^n \binom{i}{r} U_i^{k,m}$ gives the number of r -collisions. Using 1.1.(a) we find that $\mathbf{E}(S_r^{k,m}) = \frac{1}{m^{r-1}} \binom{k}{r}$.

If we regard k as a time variable (i.e.: consider the “cell occupancy process”, where the balls are distributed one after another into the cells) the first r -collisions will thus appear at times of order $t_{r,m} := (r! m^{r-1})^{1/r}$. More precisely: define the appearance time $T_{r,m}$ of the first r -collision by

$$\{T_{r,m} > k\} = \{S_r^{k,m} = 0\}$$

Then theorem 2.1 has the following corollary:

Corollary 2.2. Let $r \geq 2$ be fixed and $x > 0$. Then

$$\mathbf{P}(T_{r,m}/t_{r,m} > x) \rightarrow e^{-x^r} \quad (m \rightarrow \infty)$$

Proof. Let $x > 0$ and in the sequel $k = k(x, m) := \lceil x t_{r,m} \rceil$ and $m \rightarrow \infty$. Then $0 \leq S_r^{k,m} - U_r^{k,m} \rightarrow 0$ (since $\mathbf{E}(S_r^{k,m} - U_r^{k,m}) = \frac{1}{m^{r-1}} \binom{k}{r} (1 - (1 - \frac{1}{m})^{k-r}) \rightarrow 0$). Thus $S_r^{k,m}$ and $U_r^{k,m}$ have the same limit distribution. The conditions of 2.1,(b) are fulfilled with $a_r = x^r$. Thus $\mathbf{P}(T_{r,m} > k(x, m)) = \mathbf{P}(S_r^{k(x,m),m} = 0) \rightarrow e^{-x^r}$ \square

The limiting distribution is a Weibull distribution with form parameter r . In particular, the case $r = 2$ (the Weibull distributions with $r = 2$ are also called Rayleigh distributions) of this corollary is well known.

2.2. A (very incomplete) guide to the literature.

These classical results have been generalised and refined in many ways, and there is an abundance of literature on the classical birthday problem and its generalisations.

It is impossible to give a complete survey, we just point to some references. Modern accounts were e.g. given by Holst [13, 14] and by Camarri and Pitman [4],[3]. Diaconis and Mosteller gave in [7] in conversational style a nice general discussion of studying “coincidences”. These works contain numerous references.

Similar questions are frequently studied and interpreted in the field of “occupancy statistics”, or using “urn models”.

In classical occupancy statistics one deals with the following situation:

k distinguishable particles can be independently of each other in one of m states, there is no restriction on the number of particles in a state, each allocation of the particles into the cells is equiprobable.

It is clear from the above that the limit theorem for the r -repetition times are simple consequences of Poisson limits for certain occupancy functionals. Therefore such limit theorems are frequently implicit in certain poisson limit theorems in occupancy statistics. The book [19] by Kolchin, Sevastyanov and Chistyakov is authoritative on occupancy statistics (allocation of particles into cells).

For the application of urn models the book [15] by Johnson and Kotz is a comprehensive source.

Surprisingly, the special question of “collision” times (as opposed to “repetition” times) apparently has to the best of the authors knowledge not been dealt with directly in the statistical literature so far.

There is a considerable amount of cryptographic literature on collision attacks. “Collision attacks” in their diverse forms (e.g. “classical”, “meet in the middle” etc.) are a basic cryptanalytic tool and appeared already in the beginning of public research on cryptography (e.g [5],[10]). Also, from the beginning of hash function design, “collision resistance” has been a primary goal. However, predictions for the effort of such attacks invariably used the “random mapping assumption” (aka “random oracle model”).

A treatment of the classical birthday problem for $r = 2$ is given in many textbooks.

Stinson[25] analysed preimage-, 2nd -preimage and collision attacks in the random oracle model (using “drawing without replacement”), and reductions

between the diverse attacks.

Criticism of the random mapping assumption was formulated only relatively recently.

Bellare and Kohno[2] were the first to point out that the random mapping assumption needs justification. They discussed collision resistance for the cases of a fixed/ uniform random mapping and drawing with replacement (the model is explained in detail below), introduced a balance measure (essentially a variant of the χ^2 -statistic, as we shall see below) and were mainly interested in bounds for the probabilities $\mathbf{P}(K_2 \leq k)$ of the collision time K_2 in terms of their balance measure. (They also treat bounds for the expectation of K_2 in an appendix). However, their bounds are not particularly tight. Much better bounds were obtained by Wiener [30], who considered “drawing without replacement” and treated the cases of uniform and “multinomial” random functions (explained below) as well as concrete functions.

Laccetti and Schmid [20] generalised Stinson’s work to concrete mappings, gave exact expressions for the success probabilities of suitably randomised algorithms, and used the theory of majorization to characterise the behaviour of the success probabilities in terms of the uniformity of the mapping.

Multi-collision attacks were considered less often.

Preneel in his Ph.D. dissertation [22] discussed the classical r -fold birthday problem, and essentially rederived independently some of von Mises’ results. This case was once more analysed by Suzuki, Tonien, Kurosawa and Toyota [27], who showed that the $m^{(r-1)/r}$ effort is correct only for small fixed r and that asymptotically $\mathbf{P}(R_r \leq (r!)^{1/r} m^{(r-1)/r}) \geq \frac{1}{2}$ if $(r!/n)^{1/r} \approx 0$.

Nandi and Stinson [21] derive the effort for r -collision attacks on uniform random mappings from an approximation given in [7].

From the practical side, Joux’s[16] spectacular multi-collision attack on cascaded constructions of iterated hash functions demonstrated highly non-random behaviour in a class of hash-function constructions. This attack has been generalised in several ways.

Finally, Ramanna and Sarkar [23] generalised Bellare and Kohno’s work to the case of multi-collisions, along with some major improvements.

In all fairness it must be stated that almost all of these works plainly ignore most of the considerable statistical literature on the subject.

3. CONTRIBUTIONS OF THIS WORK

In contrast to the above mentioned works we give a treatment (apparently the first) of the collision times via generating functions and integral representations. We consider all cases of interest (i.e. drawing with resp. without replacement and concrete as well as random mappings) and demonstrate that using the classical apparatus of occupancy statistics one can easily answer all questions of interest in a very precise manner. We obtain sharp estimates for the expectation of the collision resp. repetition times, and for the first time obtain (under natural conditions) limit theorems for their distributions.

The results provide precise conditions under which the cryptographic folklore-beliefs are valid.

4. STOCHASTIC MODEL AND FIRST ORIENTATION

4.1. The stochastic model. Since the structure of the sets \mathcal{D} resp. \mathcal{R} is irrelevant for the generic collision search we let w.l.o.g in the sequel $\mathcal{D} = \{1, \dots, n\}$ and $\mathcal{R} = \{1, \dots, m\}$.

The random production of preimages of h can obviously be interpreted as “drawing” from an urn which contains resp. $x_i = |h^{-1}(\{i\})|$ balls of “colour” i .

Consider the following situation:

- an urn contains n distinguishable balls of m different colours, namely x_i (distinguishable) balls of colour i , $x_1 + x_2 + \dots + x_m = n$
- balls are drawn (1) without replacement (2) with replacement from this urn, each draw costing one time unit
- in case (1) after each draw the next ball is chosen with uniform probability among the remaining balls, in case (2) the next ball is chosen with uniform probability among all balls.
- the sampling is continued until the the random time point K_r resp. R_r , at which for the first time r different (resp. r) balls of the same colour have been drawn

In the case of sampling with replacement it is necessary to distinguish between “repetitions” (an image is hit r times, but possibly from a repeated preimage) and (true) multi-collisions.

Note on use of the word “collision”. In standard use of language a second appearance during a drawing process (a duplicate) is interchangeably referred to as a “match”, a “coincidence”, a “collision” or a “repetition”. Here we use “collision” exclusively for the appearance of a “true” collision, i.e. two (resp. r pairwise) different domain points with the same image point, and use “repetition” for the second (resp. r -th) appearance of an image point.

Relation to the classical r -birthday problem. It is well known that the classical r -birthday problem may be formulated as an urn problem:

k balls are drawn with replacement from an urn containing m different balls. How big is the chance that no ball is drawn more than $r - 1$ times?

Thus case (2) with $n = m$, $x_1 = \dots = x_m = 1$ - in the sequel called “the classical case” - covers the classical r -birthday problem. In this sense the repetition problems considered here are generalisations of the classical r -birthday problem. Note however that in the classical setting no collisions (in the sense above) are possible.

4.2. Generating functions for the occupancy numbers at time k .

4.2.1. Fixed configuration. Let us call the set (x_1, \dots, x_m) the “configuration” of h and let $Y_1(k), \dots, Y_m(k)$ be the random variables $Y_i(k) :=$ “number of **different** balls of colour i ” that have been drawn (at time k).

Let further $Z_1(k), \dots, Z_m(k)$ be the random variables $Z_i(k) :=$ “number of balls of colour i ” that have been drawn (at time k).

(In case 1 $Z_i(k)$ coincides with $Y_i(k)$ as only different balls are drawn when

drawing without replacement).

The generating function for these variables can be derived by direct combinatorial arguments.

Theorem 4.1. (1) In case 1 (drawing without replacement) the generating function of (the joint distribution of) $Y_1^{(1)}(k), \dots, Y_m^{(1)}(k)$ is given by:

$$(4.1) \quad \mathbf{E} t_1^{Y_1^{(1)}(k)} \dots t_m^{Y_m^{(1)}(k)} = \frac{k! (n-k)!}{n!} [t^k] (1 + t t_1)^{x_1} \dots (1 + t t_m)^{x_m}$$

(2a) In case 2 (drawing with replacement) the generating function of (the joint distribution of) $Y_1^{(2)}(k), \dots, Y_m^{(2)}(k)$ is given by:

$$(4.2) \quad \mathbf{E} t_1^{Y_1^{(2)}(k)} \dots t_m^{Y_m^{(2)}(k)} = \frac{k!}{n^k} [t^k] (1 + (e^t - 1) t_m)^{x_1} \dots (1 + (e^t - 1) t_m)^{x_m}$$

(2b) In case 2 (drawing with replacement) the generating function of (the joint distribution of) $Z_1(k), \dots, Z_m(k)$ is given by:

$$(4.3) \quad \mathbf{E} t_1^{Z_1(k)} \dots t_m^{Z_m(k)} = \frac{k!}{n^k} [t^k] e^{t t_1 x_1} \dots e^{t t_m x_m}$$

Proof. (1) it is easily argued that

$$\mathbf{P}(Y_1^{(1)}(k) = j_1, \dots, Y_m^{(1)}(k) = j_m) = \frac{\binom{x_1}{j_1} \dots \binom{x_m}{j_m}}{\binom{n}{k}}$$

(i.e. the joint distribution is the m -dim. hypergeometric distribution with parameters n, k and x_1, \dots, x_m). The generating function follows.

(2a) we have

$$\mathbf{P}(Y_1^{(2)}(k) = j_1, \dots, Y_m^{(2)}(k) = j_m) = \frac{1}{n^k} \cdot \binom{x_1}{j_1} \dots \binom{x_m}{j_m} \cdot \text{Sur}(k, j_1 + \dots + j_m)$$

where $\text{Sur}(k, r)$ denotes the number of surjective mappings from $\{1, \dots, k\}$ onto $\{1, \dots, r\}$.

It is known that $\text{Sur}(k, r) = k! [t^k] (e^t - 1)^r$ (since a such a surjective mapping corresponds uniquely to an ordered partition of $\{1, \dots, k\}$ in r into non-empty subsets, and $e^t - 1$ is the exponential generating function for non-empty sets). The generating function follows.

(2b) the generating function follows from the fact that

$$\mathbf{P}(Z_1(k) = j_1, \dots, Z_m(k) = j_m) = \frac{1}{n^k} \cdot \binom{k}{j_1, \dots, j_m} x_1^{j_1} \dots x_m^{j_m}$$

(i.e. the joint distribution of $(Z_1(k), \dots, Z_m(k))$ is the multinomial distribution with parameters k and $p_1 := \frac{x_1}{n}, \dots, p_m := \frac{x_m}{n}$.) \square

4.2.2. Random configuration. Now let us now consider the following two-stage random experiment:

- (1) in the first stage the urn is filled at random with the balls of different colours
- (2) in the second stage the balls are drawn from the urn

i.e. the numbers x_i are realisations of random variables X_i , where $X_1 + \dots + X_m = n$, and conditional on $X_1 = x_1, \dots, X_m = x_m$ the situation above is given.

Let $g_{(X_1, \dots, X_m)}(t_1, \dots, t_m) := \mathbf{E} t_1^{X_1} \dots t_m^{X_m}$ denote the generating function of (X_1, \dots, X_m) and let $Y_1(k), \dots, Y_m(k)$ and $Z_1(k), \dots, Z_m(k)$ have the same meaning as above, but for the two-stage experiment.. Then the following is immediate:

Corollary 4.2. *If the urn is filled with a random configuration (X_1, \dots, X_m) the following statements hold*

(1) *In case 1 (drawing without replacement) the generating function of (the joint distribution of) $Y_1^{(1)}(k), \dots, Y_m^{(1)}(k)$ is given by:*

$$(4.4) \quad \mathbf{E} t_1^{Y_1^{(1)}(k)} \dots t_m^{Y_m^{(1)}(k)} = \frac{k! (n-k)!}{n!} [t^k] g_{(X_1, \dots, X_m)}(1 + t t_1, \dots, 1 + t t_m)$$

(2a) *In case 2 (drawing with replacement) the generating function of (the joint distribution of) $Y_1^{(2)}(k), \dots, Y_m^{(2)}(k)$ is given by:*

$$\mathbf{E} t_1^{Y_1^{(2)}(k)} \dots t_m^{Y_m^{(2)}(k)} = \frac{k!}{n^k} [t^k] g_{(X_1, \dots, X_m)}(1 + (e^t - 1) t_1, \dots, 1 + (e^t - 1) t_m)$$

(2b) *In case 2 (drawing with replacement) the generating function of (the joint distribution of) $Z_1(k), \dots, Z_m(k)$ is given by:*

$$\mathbf{E} t_1^{Z_1(k)} \dots t_m^{Z_m(k)} = \frac{k!}{n^k} [t^k] g_{(X_1, \dots, X_m)}(e^{t t_1}, \dots, e^{t t_m})$$

For a uniform random (n, m) -mapping the joint distribution of (X_1, \dots, X_m) is the multinomial distribution with parameters n and $p_1 = \dots, p_m = \frac{1}{m}$. For a random (n, m) -mapping where the images take independently the value i with probability p_i it is the multinomial distribution with parameters n and p_1, \dots, p_m . Mappings with multinomially distributed preimage sizes (X_1, \dots, X_m) will in the sequel be called “multinomial”.

Let us consider this case as an example.

Example 4.3. Let $p_1, \dots, p_m \geq 0$ with $p_1 + \dots + p_m = 1$ and let

$$g_{(X_1, \dots, X_m)}(t_1, \dots, t_m) = (t_1 p_1 + \dots + t_m p_m)^n.$$

Then for $k \leq n$

$$\mathbf{E} t_1^{Y_1^{(1)}(k)} \dots t_m^{Y_m^{(1)}(k)} = \frac{k! (n-k)!}{n!} [t^k] (1 + t(t_1 p_1 + \dots + t_m p_m))^n = (t_1 p_1 + \dots + t_m p_m)^k$$

That is, the joint distribution of $(Y_1^{(1)}(k), \dots, Y_m^{(1)}(k))$ is multinomial with parameters k and p_1, \dots, p_m . Note that for $p_1 = \dots = p_m$ this is exactly the situation of the classical birthday problem (for m birthdays). **Thus (as long as $k \leq n$) drawing without replacement from a (uniform) multinomial configuration leads to the same occupancy distribution at time k as in the setting of the classical birthday problem in the codomain.**

In other words:

sampling k times without replacement from a multinomial $n, (p_1, \dots, p_m)$ mapping produces a multinomial $k, (p_1, \dots, p_m)$ mapping, and sampling without replacement from a $n, (\frac{x_1}{n}, \dots, \frac{x_m}{n})$ multinomial random (n, m) -mapping produces for $k \leq n$ the same distribution of $(Z_1(k), \dots, Z_m(k))$ as does sampling

with replacement from a fixed (n, m) mapping with configuration (x_1, \dots, x_m) . In these cases the description by a multinomial random mapping is exact!

4.3. Notation and conventions. Let w.l.o.g. all random variables appearing in the sequel be defined on the same probability space $(\Omega, \mathcal{A}, \mathbf{P})$. The cases “drawing without” resp. “with replacement” are called “case 1” resp. “case 2” in the sequel and indicated by the use of the superscripts “1” resp. “2”. The collision degree r is a fixed (small) number $r \geq 2$, $r = 2$ is the most interesting case.

We use the convention $\inf(\emptyset) = \infty$ and let $K_r^{(1)}, K_r^{(2)}$ resp. $R_r : \Omega \longrightarrow \mathbf{N} \cup \{\infty\}$ be the random variables

$$K_r^{(1)}(\omega) := \inf\{k \geq 1 : \exists i \in \{1, \dots, m\} \text{ s.th. } Y_i^{(1)}(k)(\omega) \geq r\}$$

$$K_r^{(2)}(\omega) := \inf\{k \geq 1 : \exists i \in \{1, \dots, m\} \text{ s.th. } Y_i^{(2)}(k)(\omega) \geq r\}$$

“time of the first r -collision” when drawing without resp. with replacement

$$R_r(\omega) := \inf\{k \geq 1 : \exists i \in \{1, \dots, m\} \text{ s.th. } Z_i(k)(\omega) \geq r\}$$

“time of the first r -fold repetition” when drawing with replacement.

In case 1 (drawing without replacement) it does not make sense to draw from an empty urn. Therefore we stipulate for this case that the drawing process is stopped latest at the $(n + 1)$ -drawing (i.e. after the first observation that the urn is empty.). $K_r^{(1)}(\omega) > n$ then means that no r -collisions have appeared. To guarantee the finiteness of these waiting times we assume in the sequel that at least for one i we have $x_i \geq r$ resp. $\mathbf{P}(X_i \geq r) > 0$.

It is clear that the distributions of $K_r^{(1)}, K_r^{(2)}$ resp. R_r depend on the parameters $n, m, x = (x_1, \dots, x_m)$ resp. $n, m, \mathbf{P}_{(X_1, \dots, X_m)}$, but this dependency is for convenience suppressed from the notation.

4.4. First orientation: expected number of r -collisions at time k . For a first orientation one will compute the expected number of r -collisions at time k . With $Y_i(k)$ resp. $Z_i(k)$ as above the number of r -collisions is given by the random variables

$$S_r^{(1)}(k) := \sum_{i=1}^m \binom{Y_i^{(1)}(k)}{r} \text{ resp. } S_r^{(2)}(k) := \sum_{i=1}^m \binom{Y_i^{(2)}(k)}{r}$$

while for sampling with repetition the number of r -multi-sets with colliding image (but possibly repeated preimages) is given by

$$C_r(k) := \sum_{i=1}^m \binom{Z_i(k)}{r}$$

Let $s_{r,n} := \sum_{i=1}^m \binom{x_i}{r}$. Using the generating functions given above we find:

$$\mathbf{E}(S_r^{(1)}(k)) = \frac{(k)_r}{(n)_r} s_{r,n}$$

$$\mathbf{E}(C_r(k)) := \frac{(k)_r}{r! n^r} \sum_{i=1}^m x_i^r$$

$$\mathbf{E}(S_r)^{(2)}(k) = \left(\sum_{i=0}^r \binom{r}{i} (-1)^i \left(1 - \frac{i}{n}\right)^k \right) s_{r,n} = \left(\frac{(k)_r}{n^r} \left(1 - \frac{r(k-r)}{2n} + \dots\right) \right) s_{r,n}$$

Remark: in the case of sampling with repetition we count here an occurring r -collision only once. The corresponding r -set may of course repeatedly occur in sequence of preimages. For the case of counting with multiplicities one gets [23]:

$$\mathbf{E}(S_{r,2,multi})(k) = \frac{(k)_r}{n^r} s_{r,n}$$

Thus we have the following picture:

- (1) first r collisions resp. r -repetitions will appear at times of magnitude $t_C := n/(s_{r,n})^{1/r}$ resp. of magnitude $t_R := n/(\sum_{i=1}^m \frac{x_i^r}{r!})^{\frac{1}{r}}$.
- (2) one will hope for limit theorems if the the parameters n, m, x are varied in such a way that for $t = t_C$ (resp. $t = t_R$) $t = t(n, m, x) \rightarrow \infty$.
If the cell probabilities $p_i = \frac{x_i}{n}$ are uniformly small one will expect (on the ground of known limit theorems for weakly dependent indicator variables) expect Poisson limits for the number of r -collisions resp. r -repetitions .
- (3) the difference between drawing with. resp. without replacement will only be notable if n is relatively small or if $\sum_{i=1}^m p_i^r$ is of magnitude $\frac{1}{n^{r-1}}$.
- (4) in the case of sampling with replacement the r -repetitions will appear no later as times of magnitude $n^{\frac{r-1}{r}}$ (as by 2.1 resp. 2.2 r -repetitions of preimages will appear at this time).

5. EXACT TREATMENT OF THE COLLISION TIMES

For the formulation of generating functions we need some definitions. For $n \in \mathbf{N}, t \in \mathbf{R}$ let

$$(5.1) \quad p_r(n, t) := \sum_{i=0}^{r-1} \binom{n}{i} t^i$$

$$(5.2) \quad q_r(n, t) := \sum_{i=0}^{r-1} \frac{n^i t^i}{i!}$$

$$(5.3) \quad G_r(n, t) := \sum_{i=0}^{r-1} \binom{n}{i} t^i (1-t)^{n-i}$$

Note that for $0 \leq t \leq 1$ the function $F_r(n, t) := 1 - G_r(n, t)$ is the distribution function of the r -th largest element (the r -th order statistic) of a sample of n i.i.d. variables uniform on $[0, 1]$.

5.1. Combinatorial formulae. We clearly have:

Remark 5.1.

$$\begin{aligned}\mathbf{P}(K_r > k) &= \mathbf{P}(Y_1(k) \leq r-1, \dots, Y_m(k) \leq r-1) \quad \text{and} \\ \mathbf{P}(R_r > k) &= \mathbf{P}(Z_1(k) \leq r-1, \dots, Z_m(k) \leq r-1)\end{aligned}$$

5.1.1. *Fixed mapping.* Let again be $h : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ a mapping with preimage cardinalities $x_i = |h^{-1}(\{i\})|$.

From the generating functions of the cell occupancies given above we get exact combinatorial expressions for the probabilities in question.

Theorem 5.2.

$$(5.4) \quad \mathbf{P}(K_r^{(1)} > k) = \frac{k! (n-k)!}{n!} [t^k] \prod_{i=1}^m p_r(x_i, t)$$

$$(5.5) \quad \mathbf{P}(K_r^{(2)} > k) = \frac{k!}{n^k} [t^k] \prod_{i=1}^m p_r(x_i, e^t - 1)$$

$$(5.6) \quad \mathbf{P}(R_r > k) = \frac{k!}{n^k} [t^k] \prod_{i=1}^m q_r(x_i, t)$$

If we denote the k -th elementary symmetric function of the variables x_1, \dots, x_m by $Sym_k(x_1, \dots, x_m)$ and the number of surjective mappings of a k -element set onto a d element set by $Sur(k, d)$ we thus have in particular for $r = 2$

Corollary 5.3. *For $r = 2$*

$$(5.7) \quad \mathbf{P}(K_2^{(1)} > k) = \frac{k! (n-k)!}{n!} Sym_k(x_1, \dots, x_m)$$

$$(5.8) \quad \mathbf{P}(K_2^{(2)} > k) = \frac{1}{n^k} \sum_{d=0}^k Sur(k, d) Sym_d(x_1, \dots, x_m)$$

$$(5.9) \quad \mathbf{P}(R_2 > k) = \frac{k!}{n^k} Sym_k(x_1, \dots, x_m)$$

Since $x_1 + \dots + x_m = n$, and since we require that at least one x_i be $\geq r$, the products expressing the different generating functions above give polynomials in t with degree $\leq n-1$. In particular, in case (1) $\mathbf{P}(K_r > n) = 0$ and in case (2) $\mathbf{P}(R_r > n) = 0$.

The explicit form of the generating functions makes it possible to prove some “intuitively obvious” properties. We consider two such intuitions.

Firstly one expects that r -collision search becomes harder the smaller the individual preimage sizes are. The next lemma shows this intuition to be true in a very strong sense.

Lemma 5.4. (*stochastic ordering over configurations*)

- (1) if in a configuration (x_1, \dots, x_m) there are images i, j s.th. $r \leq x_i < x_j - 1$, then the probabilities $\mathbf{P}(K_r > k)$ can only increase if x_i is replaced by $x_i + 1$ and x_j is replaced by $x_j - 1$.
- (2) if in a configuration (x_1, \dots, x_m) there are images i, j s.th. $0 \leq x_i < x_j - 1$, then the probability $\mathbf{P}(R_r > k)$ can only increase if x_i is replaced by $x_i + 1$ and x_j is replaced by $x_j - 1$, or if each is replaced by $(x_i + x_j)/2$.

Proof. (1) let $x, y \in \mathbf{N}$, $r \leq x \leq y - 1$. Using the recursion $p_r(n, t) = p_r(n - 1, t) + tp_{r-1}(n - 1, t)$ it is not hard to show that

$$p_r(x, t)p_r(y, t) - p_r(x+1, t)p_r(y-1, t) = t^r \left(\binom{x}{r-1} p_{r-1}(y-1, t) - \binom{y-1}{r-1} p_{r-1}(x, t) \right)$$

The non-zero coefficients of t on the rhs are $\binom{y-1}{j} \binom{x}{r-1} - \binom{x}{j} \binom{y-1}{r-1}$, $0 \leq j \leq (r-1)$ are thus nonnegative.

(2) let $x, y \in \mathbf{R}_+$, $x < y$. We show that $[t^k]q_r(xt)q_r(yt) \leq [t^k](q_r((x+y)/2)t)^2$. It is easy to see that equality holds for $k \leq r-1$ and $k > 2r-2$. Let $r \leq k \leq 2r-2$. We have

$$k! [t^k]q_r(xt)q_r(yt) = (x+y)^k - \sum_{i=0}^{k-r} \binom{k}{i} (x^i y^{k-i} + y^i x^{k-i})$$

For fixed sum $s = x + y$ the function $x \mapsto f(x) := \sum_{i=0}^{k-r} \binom{k}{i} (x^i y^{k-i} + y^i x^{k-i})$ has the derivative $f'(x) = (k-r+1) \binom{k}{r} (x^{k-r+1}(s-x)^r - (s-x)^{k-r+1}x^r)$. Thus $x \mapsto f(x)$ is strictly decreasing (resp. increasing) on $[0, s/2]$ (resp. $[s/2, s]$), attaining its minimum at $x = s/2$. \square

The r -collision times are therefore stochastically largest when the preimage sizes $\geq r$ are as uniform as possible, and the r -repetition time is stochastically largest when the preimage sizes are as uniform as possible.

Secondly one expects that collisions are easier to find when it is guaranteed that the sampled domain points are mutually different, i.e. if sampling without replacement is used. The following lemma shows that this is indeed true.

Lemma 5.5. (*stochastic ordering between the different waiting times*)

1. For $k \in \mathbf{N}$ and $r \geq 2$

$$\mathbf{P}(K_r^{(2)} > k) \geq \mathbf{P}(K_r^{(1)} > k) \text{ and } \mathbf{P}(K_r^{(2)} > k) \geq \mathbf{P}(R_r > k)$$

2. For $r = 2, k \in \mathbf{N}$ also

$$\mathbf{P}(K_2^{(1)} > k) \geq \mathbf{P}(R_2 > k)$$

Proof. 1. by the formulae in theorem 4.2 above

$$\mathbf{P}(K_r^{(2)} > k) = \frac{1}{n^k} \sum_{d=0}^k \text{Sur}(k, d) \binom{n}{d} \mathbf{P}(K_r^{(1)} > d) \geq \mathbf{P}(K_r^{(1)} > k) \left(\frac{1}{n^k} \sum_{d=0}^k \text{Sur}(k, d) \binom{n}{d} \right) = \mathbf{P}(K_r^{(1)} > k)$$

where we have used that $\sum_{d=0}^k \text{Sur}(k, d) \binom{n}{d} = n^k$.

2.: since $p_2(x, t) = 1 + xt = q_2(xt)$ the formulae above give

$$\mathbf{P}(R_2 > k) = \frac{n!}{(n-k)!n!} \mathbf{P}(K_2^{(1)} > k)$$

Thus R_2 is distributed as the $\min(T, K_2^{(1)})$ where T is independent of $K_2^{(1)}$, and distributed as the waiting time for the first 2-collision of preimages. \square

In case 2 the numbers $\binom{n}{d} \frac{\text{Sur}(k,d)}{n^d} =: \mathbf{P}(I^{(k,n)} = d)$ give the probabilities that the image of the (uniform) random mapping $\{1, \dots, k\} \rightarrow \mathcal{D}$ given by $i \mapsto D_i$ has cardinality d . Using this r.v. $I^{(k,n)}$ we have $\mathbf{P}(K^{(2)} > k \mid I^{(k,n)} = d) = \mathbf{P}(K^{(1)} > d)$, and

$$\mathbf{P}(K^{(2)} > k) = \sum_{d=0}^k \mathbf{P}(K^{(1)} > k) \mathbf{P}(I^{(k,n)} = d)$$

These relations hold for any fixed configuration, and thus also for random configurations.

If we denote “ X is stochastically larger than Y ” by $Y \preceq X$ we may summarise lemma 2 as: For $r = 2$ we have $R_2 \preceq K^{(1)} \preceq K^{(2)}$, and for $r \geq 3$ we have $R_r \preceq K_r^{(2)}$ and $K_r^{(1)} \preceq K_r^{(2)}$. The following example shows that in general for $r \geq 3$ no stochastic ordering between $K_r^{(1)}$ and R_r exists:

Example 5.6. Let $r \geq 3, n = r + 1, m = 2, x_1 = 1, x_2 = r$. Then on the one hand

$$\mathbf{P}(K_r^{(1)} = r) = \frac{1}{r+1} < \frac{1+r^r}{(r+1)r} = \mathbf{P}(R_r = r)$$

and therefore $\mathbf{P}(K_r^{(1)} > r) > \mathbf{P}(R_r > r)$. On the other hand $\mathbf{P}(K_r^{(1)} > r+1) = 0$ but $\mathbf{P}(R_r > r+1) \geq \mathbf{P}(R_r > 2r-2) > 0$.

5.1.2. *Random configurations.* For multinomial (n, m) -random mappings (with parameters n and p_1, \dots, p_m) we find:

Theorem 5.7.

$$(5.10) \quad (\text{for } k \leq n) \quad \mathbf{P}(K_r^{(1)} > k) = k! [t^k] \prod_{i=1}^m q_r(p_i t)$$

$$(5.11) \quad \mathbf{P}(K_r^{(2)} > k) = \sum_{d=0}^k \mathbf{P}(K_r^{(1)} > d) \mathbf{P}(I^{(k,n)} = d)$$

Proof. From 4.3 we know that in case 1 the joint distribution of $(Y_1^{(1)}(k), \dots, Y_m^{(1)}(k))$ is for $k \leq n$ the multinomial distribution with parameters k and p_1, \dots, p_m . Thus

$$\mathbf{E} t_1^{Y_1^{(1)}(k)} \dots t_m^{Y_m^{(1)}(k)} = (t_1 p_1 + \dots + t_m p_m)^k = k! [t^k] \prod_{i=1}^m e^{p_i t_i t}$$

The representation above follows. \square

Again we note the case $r = 2$ separately:

Corollary 5.8.

$$(5.12) \quad \mathbf{P}(K_2^{(1)} > k) = k! \text{Sym}_k(p_1, \dots, p_m)$$

$$(5.13) \quad \mathbf{P}(K_2^{(2)} > k) = \frac{1}{n^k} \sum_{d=0}^k \text{Sur}(k, d) \frac{n!}{(n-d)!} \text{Sym}_d(p_1, \dots, p_m)$$

$$(5.14) \quad \mathbf{P}(R_2 > k) = \frac{k!}{n^k} \frac{n!}{(n-k)!} \text{Sym}_k(p_1, \dots, p_m)$$

Some remarks are in order:

- (1) r -collisions can only occur if a cell occupancy $x_i \geq r$ exists, and the appearance of the terms $\binom{x_i}{r}$ in the formulae for the collision times (for concrete mappings) reflects this (the formulae for the repetition times contain the terms x_i^r instead). (This was earlier remarked by Wiener [30] and Ramanna and Sarkar [23]).
- (2) the consideration of random configurations involves an “averaging” over an ensemble of mappings. It is then clear that the description by a random mapping is not appropriate for “improbable” mappings. E.g. if $n = m$ and h is a permutation no collisions are possible. It turns out, however, that the characteristics which determine the collision behaviour have under certain conditions a weak limit for “very large” random mappings (i.e. have values of the same order of magnitude for “almost all” mappings). In these cases we may say that random mappings have a typical collision behaviour.
- (3) probability bounds for the collision times: since we are interested in limit theorems rather than probability bounds we shall not pursue this here. But we note that the concrete representation of the probabilities as coefficients of power series makes it possible to use the saddle point method to derive very good estimates for these probabilities (in the same way as Good [11] did for the multinomial distribution).

5.2. The generating functions for the collision/repetition times. There are several methods to treat the distributions of these waiting times. We use (integral representations) for the generating functions of the probabilities $\mathbf{P}(K_r > k)$ resp. $R_r > k$, because these are particularly near at hand, given the explicit representation for the coefficients.

Let in the sequel

$$\begin{aligned} g_r^{(1)}(u) &:= \sum_{k=0}^{\infty} u^k \mathbf{P}(K_r^{(1)} > k) \\ g_r^{(2)}(u) &:= \sum_{k=0}^{\infty} u^k \mathbf{P}(K_r^{(2)} > k) \\ h_r(u) &:= \sum_{k=0}^{\infty} u^k \mathbf{P}(R_r > k) \end{aligned}$$

(Recall the convention $\mathbf{P}(K^{(1)} > n+1) = 0$.)

These series are clearly convergent for $|u| < 1$, and we have

$$g_r^{(1)}(1) = \mathbf{E}(K_r^{(1)}), \quad g_r^{(2)}(1) = \mathbf{E}(K_r^{(2)}), \quad h_r(1) = \mathbf{E}(R_r).$$

Theorem 5.9.

$$(5.15) \quad g_r^{(1)}(u) = (n+1) \int_0^1 (1-t)^n \prod_{i=1}^m p_r(x_i, \frac{ut}{1-t}) dt$$

$$(5.16) \quad = (n+1) \int_0^\infty e^{-(n+1)s} \prod_{i=1}^m p_r(x_i, u(e^s - 1)) ds$$

$$(5.17) \quad g_r^{(2)}(u) = n \int_0^\infty e^{-ns} \prod_{i=1}^m p_r(x_i, e^{us} - 1) ds$$

$$(5.18) \quad h_r(u) = n \int_0^\infty e^{-ns} \prod_{i=1}^m q_r(x_i u s) ds$$

Proof. Using the well known relations $\int_0^1 t^a (1-t)^b dt = \frac{a!b!}{(a+b+1)!}$ and $\int_0^\infty s^k e^{-s} = k!$ this follows immediately from the representation in Theorem 5.2 above. Note that summation and integration may be freely interchanged, since all summands are nonnegative. \square

5.3. Expectation of the waiting times. For the expectations we have thus the following expressions

Proposition 5.10.

$$(5.19) \quad \mathbf{E}(K_r^{(1)}) = (n+1) \int_0^1 (1-t)^n \prod_{i=1}^m p_r(x_i, \frac{t}{1-t}) dt$$

$$(5.20) \quad = (n+1) \int_0^\infty e^{-(n+1)s} \prod_{i=1}^m p_r(x_i, (e^s - 1)) ds$$

$$(5.21) \quad \mathbf{E}(K_r^{(2)}) = n \int_0^\infty e^{-ns} \prod_{i=1}^m p_r(x_i, e^s - 1) ds$$

$$(5.22) \quad \mathbf{E}(R_r) = n \int_0^\infty e^{-ns} \prod_{i=1}^m q_r(x_i s) ds$$

Some remarks:

- (1) As $p_r(x, t) = (1+t)^x$ for $x \leq r-1$ we may rewrite the expectations of the collision times using $M_r := \{i : x_i \geq r\}$ as follows

$$\mathbf{E}(K_r^{(1)}) = (n+1) \int_0^1 \prod_{i \in M_r} G_r(x_i, t) dt$$

$$\mathbf{E}(K_r^{(2)}) = n \int_0^\infty \prod_{i \in M_r} G_r(x_i, 1 - e^{-t}) dt$$

The quotients $\mathbf{E}(K_r^{(1)})/(n+1)$ and $\mathbf{E}(K_r^{(2)})/n$ thus depend only on the x_i with $x_i \geq r$. In contrast $\mathbf{E}(R_r)/n$ depends on all x_i with $x_i > 0$.

- (2) if T_1, \dots, T_m are independent $B(r, x_i+1-r)$ -variables we have $\mathbf{E}(K_r^{(1)}) = (n+1) \mathbf{E}(\min\{T_1, \dots, T_m\})$. Similarly, if T_1, \dots, T_m are independent,

and T_i is distributed as the r -th order statistic of x_i independent exponential variables with mean 1, we have $\mathbf{E}(K_r^{(2)}) = n \mathbf{E} \min\{T_1, \dots, T_m\}$. Finally, if T_1, \dots, T_m are independent $\Gamma(x_i, r)$ distributed we have $\mathbf{E}(R_r) = n \mathbf{E} \min\{T_1, \dots, T_m\}$ (this was earlier shown by Holst [14]).

- (3) for the classical case the representation (5.22) is a well known result due to Klamkin and Newman ([17]). The general multinomial case was given in [8] and [14].

In simple cases the integrals can be evaluated explicitly. In the sequel $B(a, b)$ denotes the Beta function.

Example 5.11. Let $x_i \leq r$ for all i , and $a := |\{i : x_i = r\}| \geq 1$. Then

$$\begin{aligned} \mathbf{E}(K_r^{(1)}) &= (n+1) \int_0^1 (1-t^r)^a dt = \frac{n+1}{r} B\left(\frac{1}{r}, 1+a\right) = (n+1) \frac{a! r^a}{\prod_{i=1}^a (1+ir)} \approx \Gamma\left(1 + \frac{1}{r}\right) \frac{n+1}{(1+a)^{1/r}} \\ \mathbf{E}(K_r^{(2)}) &= n \int_0^1 (1-t^r)^a \frac{1}{1-t} dt = \frac{n}{r} \left(\sum_{i=1}^{r-1} B\left(\frac{i}{r}, a+1\right) \right) \end{aligned}$$

In the case $a = 1$ of only one possible r -collision thus

$$\mathbf{E}(K_r^{(1)}) = \frac{r}{r+1} (n+1) \text{ and } \mathbf{E}(K_r^{(2)}) = n \left(1 + \frac{1}{2} + \dots + \frac{1}{r}\right)$$

Note that this example includes the exact solutions for the case of “ r -regular” functions, where r -regular means that $a = m$, $n = mr$.

Example 5.12. Let $x_i \geq r$ for only one i , $x_i = x$. Then

$$\mathbf{E}(K_r^{(1)}) = r \frac{n+1}{x+1} \text{ and } \mathbf{E}(K_r^{(2)}) = n \sum_{i=0}^{r-1} \frac{1}{x-i}$$

In particular, in the case of a constant mapping ($x = n$) thus

$$\mathbf{E}(K_r^{(1)}) = r \text{ and } \mathbf{E}(K_r^{(2)}) = r + \sum_{i=1}^{r-1} \frac{i}{n-i}$$

Proposition 5.13. (asymptotic expansion in the classical case)

Let $n = m$, $x_1 = x_2 = \dots = x_m = 1$. Then $\mathbf{E}(R_r)/n$ has an asymptotic expansion in powers of $n^{-1/r}$.

Proof. (Sketch) By Klamkin’s and Newman’s formula

$$\mathbf{E}(R_r) = n \int_0^\infty (q_r(y) e^{-y})^n dy =: n I_r(n)$$

The substitution $t = (r!(y - \log(q_r(y))))^{1/r}$ transforms $I_r(n)$ to

$$I_r(n) = \int_0^\infty e^{-n \frac{t^r}{r!}} \frac{t^{r-1}}{y(t)^{r-1}} q_r(y(t)) dt$$

Since $y(t) > t$ for $t > 0$ (comp. Lemma 8.3) and since $t \mapsto q_r(t)/t^{r-1}$ is decreasing

$$I_r(n) < \int_0^\infty e^{-n \frac{t^r}{r!}} q_r(t) dt = \frac{1}{r} \sum_{i=0}^{r-1} \frac{1}{i!} \left(\frac{r!}{n}\right)^{(i+1)/r} \Gamma\left(\frac{i+1}{r}\right)$$

Further, $t \mapsto \frac{t^{r-1}}{y(t)^{r-1}} q_r(y(t)) =: g_r(t)$ is analytic in a neighbourhood of 0, say $g_r(t) = \sum_{i=0}^{\infty} a_i(r) t^i$. An application of Laplace's method (e.g. [6], chap. 4) now gives

$$I_r \sim \frac{1}{r} \sum_{i=0}^{\infty} a_i(r) \Gamma\left(\frac{i+1}{r}\right) \left(\frac{r!}{n}\right)^{(i+1)/r}$$

□

For instance, in the classical case

$$\begin{aligned} \mathbf{E}(R_2) &= \frac{n}{2} \left(\left(\frac{2}{n}\right)^{1/2} \Gamma\left(\frac{1}{2}\right) + \frac{2}{3} \left(\frac{2}{n}\right)^{1/1} \Gamma\left(\frac{2}{2}\right) + \frac{1}{12} \left(\frac{2}{n}\right)^{3/2} \Gamma\left(\frac{3}{2}\right) - \frac{2}{135} \left(\frac{2}{n}\right)^{4/2} \Gamma\left(\frac{4}{2}\right) + \frac{1}{864} \left(\frac{2}{n}\right)^{5/2} \Gamma\left(\frac{5}{2}\right) + \dots \right) \\ \mathbf{E}(R_3) &= \frac{n}{3} \left(\left(\frac{6}{n}\right)^{1/3} \Gamma\left(\frac{1}{3}\right) + \frac{1}{2} \left(\frac{6}{n}\right)^{2/3} \Gamma\left(\frac{2}{3}\right) + \frac{21}{80} \left(\frac{6}{n}\right)^{3/3} \Gamma\left(\frac{3}{3}\right) + \frac{7}{240} \left(\frac{6}{n}\right)^{4/3} \Gamma\left(\frac{4}{3}\right) + \frac{83}{13440} \left(\frac{6}{n}\right)^{5/3} \Gamma\left(\frac{5}{3}\right) + \dots \right) \\ \mathbf{E}(R_4) &= \frac{n}{4} \left(\left(\frac{24}{n}\right)^{1/4} \Gamma\left(\frac{1}{4}\right) + \frac{2}{5} \left(\frac{24}{n}\right)^{2/4} \Gamma\left(\frac{2}{4}\right) + \frac{17}{100} \left(\frac{24}{n}\right)^{3/4} \Gamma\left(\frac{3}{4}\right) + \frac{194}{2625} \left(\frac{24}{n}\right)^{4/4} \Gamma\left(\frac{4}{4}\right) + \frac{271}{42000} \left(\frac{24}{n}\right)^{5/4} \Gamma\left(\frac{5}{4}\right) + \dots \right) \\ \mathbf{E}(R_5) &= \frac{n}{5} \left(\left(\frac{120}{n}\right)^{1/5} \Gamma\left(\frac{1}{5}\right) + \frac{1}{3} \left(\frac{120}{n}\right)^{2/5} \Gamma\left(\frac{2}{5}\right) + \frac{5}{42} \left(\frac{120}{n}\right)^{3/5} \Gamma\left(\frac{3}{5}\right) + \frac{11}{252} \left(\frac{120}{n}\right)^{4/5} \Gamma\left(\frac{4}{5}\right) + \frac{515}{31752} \left(\frac{120}{n}\right)^{5/5} \Gamma\left(\frac{5}{5}\right) + \dots \right) \end{aligned}$$

The case $r = 2$ of this proposition is well known (cmp. [18], section 1.2.11.3 and problem 20 there), note that in the classical case $\mathbf{E}(R_2) = 1 + Q(n)$, and for $r = 3$ the first three terms were given by Holst [14], but I couldn't find the asymptotic series for higher r in the literature. (Klamkin and Newman give only the first term). Since even the encyclopaedic work [9] (where the problem is treated on p. 116) doesn't mention them, they may at least not be well known. To make the remainder $o(1)$ one has to take r terms of the asymptotic series for $\mathbf{E}(R_r)$. For example, for $r = 3$ and $n = 365$ the first term gives $\mathbf{E}(R_3) \approx 82,87442$, the first three terms give $\mathbf{E}(R_3) \approx 88,72504$ while the exact value is $\mathbf{E}(R_3) = 88,73891\dots$

Let in the sequel $\tilde{s}_r := \frac{\sum_{i=1}^m x_i^r}{r!}$, $s_r := \sum_{i=1}^m \binom{x_i}{r}$ and let w.l.o.g $x_1 := \max\{x_1, \dots, x_m\}$. We find the following bounds for the expectations:

Theorem 5.14. (*lower bounds*)

$$(5.23) \quad \mathbf{E}(K_r^{(1)}) \geq (n+1) B\left(\frac{1}{r}, 1 + s_r\right) > \Gamma\left(1 + \frac{1}{r}\right) \frac{n+1}{(s_r+1)^{1/r}}$$

$$(5.24) \quad \mathbf{E}(K_r^{(2)}) > \Gamma\left(1 + \frac{1}{r}\right) \frac{n}{(s_r)^{1/r}}$$

$$(5.25) \quad \mathbf{E}(R_r) > \Gamma\left(1 + \frac{1}{r}\right) \frac{n}{(\tilde{s}_r)^{1/r}}$$

Proof. 5.23 The left inequality follows using the inequality $G_r(x, t) \geq (1 - t^r) \binom{x}{r}$ (cmp. Lemma 8.1). The second inequality follows from Jensen's inequality: let X be a $\Gamma(s+1, 1)$ -distributed random variable, then

$$\frac{\Gamma(s+1+\frac{1}{r})}{\Gamma(s+1)} = \mathbf{E}(\sqrt[r]{X}) \leq \sqrt[r]{\mathbf{E}(X)} = \sqrt[r]{s+1}$$

5.24 follows from $G_r(x, 1 - e^{-s}) \geq e^{-\binom{x}{r} s^r}$ (for $s > 0, x \geq r$, cmp. Lemma 8.2)

5.25 follows from $q_r(t) e^{-t} > e^{-\frac{t^r}{r!}}$ (for $t > 0$, cmp. Lemma 8.3)

□

Our next aim is to find upper bounds. Let $u_r := \frac{\sum_{i \in M_r} x_i}{|M_r|}$ and $w := \min\{n, m\}$. Directly from the majorisation Lemma 5.4 we have

Proposition 5.15. (*upper bounds 1*)

$$(5.26) \quad \mathbf{E}(K_r^{(1)}) \leq (n+1) B(\frac{1}{r}, 1+u_r) \approx \Gamma(1+\frac{1}{r}) \frac{n+1}{(u_r+1)^{1/r}}$$

$$(5.27) \quad \mathbf{E}(K_r^{(2)}) \leq \frac{n}{r} \left(\sum_{i=1}^{r-1} B(\frac{i}{r}, 1+u_r) \right)$$

$$(5.28) \quad \mathbf{E}(R_r) \leq w \int_0^\infty e^{-ws} (q_r(s))^w dt \approx \Gamma(1+\frac{1}{r}) (r! w^{r-1})^{1/r}$$

These upper bounds have the disadvantage that they are not easy to compare to the lower bounds. The next theorem gives upper bounds that match the lower bounds.

Theorem 5.16. (*upper bounds 2*)

$$(5.29) \quad \mathbf{E}(K_r^{(1)}) \leq \mathbf{E}(K_r^{(2)}) < \frac{n}{s_r^{1/r}} \left(\sum_{i=0}^{r-1} \binom{x_1}{i} \frac{1}{r} \Gamma(\frac{i+1}{r}) (s_r)^{-i/r} \right)$$

$$(5.30) \quad \mathbf{E}(R_r) < \frac{n}{\tilde{s}_r^{1/r}} \left(\sum_{i=0}^{r-1} \binom{x_1}{i} \frac{1}{r} \Gamma(\frac{i+1}{r}) (\tilde{s}_r)^{-i/r} \right)$$

Proof. 5.29 (Sketch) Let $I = \mathbf{E}(K_r^{(2)})/n$ and let $L(s) := -\sum_{i=1}^m \log(G_r(x_i, s))$. $s \mapsto L(s)$ is for $s > 0$ strictly increasing. Substitute $y = (L(s)/s_r)^{1/r}$ then

$$I = \int_0^\infty e^{-s_r y^r} \frac{r s_r y^{r-1}}{L'(s(y))} dy$$

We have $L'(s) = r \sum_{i=1}^m \binom{x_i}{r} (e^s - 1)^{r-1} (p_r(x_i, e^s - 1))^{-1}$. Thus

$$\frac{L'(s)}{r s_r (e^s - 1)^{r-1}} \geq \frac{1}{p_r(x_1, e^s - 1)}$$

and

$$I \leq \int_0^\infty e^{-s_r y^r} \frac{y^{r-1}}{(e^{s(y)} - 1)^{r-1}} p_r(x_1, e^{s(y)} - 1) dy$$

Finally $y < s(y)$ (cmp. Lemma 8.2 and $s \mapsto p_r(x_1, e^s - 1)/(e^s - 1)^{r-1}$ is strictly decreasing so that

$$I \leq \int_0^\infty e^{-s_r y^{r-1}} \frac{y^{r-1}}{(e^y - 1)^{r-1}} p_r(x_1, e^y - 1) dy < \int_0^\infty e^{-s_r y^{r-1}} p_r(x_1, e^y - 1) dy$$

The result now follows by termwise integration.

For 5.30 the proof is similar. \square

Example 5.17. Let us compare the bounds from Theorem 5.14 resp. Theorem 5.16 for the case $r = 2$ to some existing bounds in the literature.

(a1) The classical birthday problem. ($n = m, x_1 = \dots x_m = 1$). Here we find

$$0 < \mathbf{E}(R_2) - \sqrt{\frac{\pi}{2} m} < 1$$

Wiener (Theorem 2) gives:

$$-\frac{2}{5} < \mathbf{E}(R_2) - \sqrt{\frac{\pi}{2}m} < \frac{8}{5}$$

while the exact best bounds are known to be ([24],[26])

$$\frac{2}{3} < \mathbf{E}(R_2) - \sqrt{\frac{\pi}{2}m} \leq 2 - \sqrt{\frac{\pi}{2}}$$

Clearly all of these bounds are comparable. In this case even the complete asymptotic expansion of $\mathbf{E}(R_2)$ is known ([18]).

(a2) The birthday problem with unequal probabilities. ($n = m, x_1 + \dots + x_m = m$). Let $p_i := \frac{x_i}{m}$ and let $\beta(p) := \frac{1}{\sum_{i=1}^m p_i^2}$, $p_1 := \max\{p_i\}$. Here we find

$$0 < \mathbf{E}(R_2) - \sqrt{\frac{\pi}{2}\beta(p)} < p_1 \beta(p)$$

Wiener (Theorem 4) gives:

$$\sqrt{\frac{\pi}{2}\beta(p)} - \frac{2}{5} < \mathbf{E}(R_2) < 2\sqrt{\beta(p)}$$

Here the lower bounds are comparable while our upper bound is clearly better.

(b) The collision time for a concrete (n, m) - function. Here we find

$$\frac{n+1}{\sqrt{s_2+1}} \frac{\sqrt{\pi}}{2} < \mathbf{E}(K_2^{(1)}) < \frac{n}{\sqrt{s_2}} \frac{\sqrt{\pi}}{2} + \frac{nx_1}{2s_2}$$

while Wiener (Theorem 8) gives for $n > m \geq 1$, translated into our notation:

$$(e-2)\sqrt{\frac{n(n-1)}{2s_2}} < \mathbf{E}(K_2^{(1)}) \leq 2\sqrt{\frac{n(n-1)}{2s_2}}$$

Here both our bounds are preferable.

Again some remarks are in order:

- (1) observe that the bounds in Theorem 5.14 resp. Theorem 5.16 are very close in the sense : upper bound = lower bound + terms of at most the same order. The expectations of K_r resp. R_r are always of the order $\frac{n}{(s_r)^{1/r}}$ resp. $\frac{n}{(\tilde{s}_r)^{1/r}}$.
- (2) the expectation of the r -collision time for a fixed configuration with given s_r is comparable to the expectation of the r -collision time of a uniform random mapping with “effective” image size $m_r = \frac{n^r}{s_r}$ (this was for $r = 2$ already remarked by Wiener). In the sequel we will see that this analogy goes very far.
- (3) the expectations of the r -collision times are always of the same order of magnitude
- (4) in contrast, even the orders of magnitude of $\mathbf{E}(K_r)$ and $\mathbf{E}(R_r)$ can be different. The reason is that every $x_i > 0$ adds to \tilde{s}_r while only the $x_i \geq r$ add to s_r . While the r -repetition time can maximal be of order $(\min\{m, n\})^{(r-1)/r}$, the r -collision times can be of order n .

6. LIMIT THEOREMS

What is the typical shape of the distribution of the waiting times for large domains/codomains? This question is answered by limit theorems. We consider in the sequel a sequence (h_N) of mappings with corresponding parameters $(n, m, (x_i)) = (n(N), m(N), (x_i(N)))$ varying with N (it is clear that the distributions only depend on these parameters), and the corresponding waiting time distributions.

For the formulation we assume w.l.o.g. that

$$x_1 \geq x_2 \geq x_3 \geq \dots$$

It will become apparent that limit theorem can conveniently be formulated using the following characteristics :

$$s_r := \sum_{i=1}^m \binom{x_i}{r}, \quad m_r = \frac{n^r}{r! s_r} \quad \text{and} \quad \rho_i := \left(\frac{x_i}{s_r} \right)^{1/r}$$

“Asymptotical” means: $m_r(N) \rightarrow \infty$ and/or $s_r(N) \rightarrow \infty$ as $N \rightarrow \infty$.
(In particular in all asymptotical considerations $n(N) \rightarrow \infty$.)

Theorem 6.1. *(asymptotical distribution of the collision times)*

Let $N \rightarrow \infty$ and assume that for each i the limit $\rho_i = \lim \rho_i(N)$ exists. Then limiting distributions of the collision times exist and are as follows:

- (1) if $s_r(N) \rightarrow \sigma < \infty, m_r(N) \rightarrow \infty$ we have :
- asymptotically, there are only finitely many i with $x_i \geq r$, for each of these i the limit $\lim x_i(N) = x_i < \infty$ exists and G

$$(a) \quad \mathbf{P}(K_r^{(1)} > nt) \rightarrow \prod_i G_r(x_i, t) \quad \text{for } 0 \leq t < 1$$

$$(b) \quad \mathbf{P}(K_r^{(2)} > nt) \rightarrow \prod_i G_r(x_i, 1 - e^{-t}) \quad \text{for } 0 \leq t < \infty$$

- (2) if $s_r(N) \rightarrow \infty, m_r(N) \rightarrow \infty$ we have (in both cases):

$$\mathbf{P}(K_r > (m_r)^{(r-1)/r} t) \rightarrow e^{-(1 - \sum_i \rho_i^r) t^r / r!} \prod_i e^{-\rho_i t} q_r(\rho_i t) \quad \text{for } 0 \leq t < \infty$$

- (3) if $s_r(N) \rightarrow \infty, m_r(N) \rightarrow \lambda < \infty$ we have (in both cases) :

for each i the limit $\lim \frac{x_i(N)}{n(N)} =: p_i$ exists, $\sum_i p_i = 1$ and for each $k \in \mathbf{N}$:

$$\mathbf{P}(K_r > k) \rightarrow k! [t^k] \prod_i q_r(p_i t) e^{-p_i t}$$

Proof. 1.(a) suppose $\lim \rho_i(N)$ exists for each i and that $s_r(N) \rightarrow \sigma < \infty$. Let $h_r(N) := \max\{i : x_i(N) \geq r\}$ the number of higher occupied cells, let

$a_r(N) := \sum_{i=1}^{h_r(N)} x_i(N)$ the number of balls in higher occupied cells and let

$$H_N(t) := \prod_{i=1}^{m(N)} p_r(x_i(N), t) (1+t)^{-x_i(N)}$$

Since $\sigma < \infty$ asymptotically there are only finitely many i with $x_i \geq r$. Thus $h_r = \lim h_r(N)$ exists and is finite, and for each $i \leq h_r$ the limit $x_i(N)$ exists and is finite. Thus there is an N_0 s.th. $x_i(N)$ is constant for $i \leq h_r$ and $N \geq N_0$. Hence $a_r(N) =: a_r$ is also constant for $N \geq N_0$. For $N \geq N_0$ then $Q_N(t) := H_N(\frac{t}{1-t})$ is a polynomial of degree a_r in t and we have

$$\mathbf{P}(K^{(1)} > k) = \frac{k! (n-k)!}{n!} [x^k] Q_N\left(\frac{x}{1+x}\right) (1+x)^n = \sum_{i=0}^{a_r} q_i \binom{k}{i} \frac{i! (n-i)!}{n!}$$

where the coefficients q_i of Q_N depend only on the x_i with $x_i \geq r$ and hence are constant for $N > N_0$. For $\frac{k}{n} \rightarrow t \in (0, 1)$ the quotients of the binomial coefficients converge to corresponding powers of t . Thus

$$\mathbf{P}(K_r^{(1)} > nt) \rightarrow Q(t) = H\left(\frac{t}{1-t}\right) \quad (n \rightarrow \infty)$$

The proof for (b) is analogous.

(2)(3) Let $Q_N(t) := \prod_{i=1}^{m(N)} G_r(x_i(N), t)$ (so that $1 - Q_N(t)$ is the distribution function of $\min\{X_1, \dots, X_m\}$ where the X_i are independent, and X_i is distributed as the r -th order statistic of x_i independent variables uniform on $[0, 1]$). and let $T_r^{(1)}(N)$ resp. $T_r^{(2)}(N)$ be random variables with $\mathbf{P}(T_r^{(1)}(N) > t) = Q_N(\frac{t}{1-t})$ resp. $\mathbf{P}(T_r^{(2)}(N) > t) = Q_N(1 - e^{-t})$. We show that the limits of the distributions of $T_r^{(1)}(N)$ resp. $T_r^{(2)}(N)$ appear as limits of the distributions of $K_r^{(1)}(N)$ resp. $K_r^{(2)}(N)$ (thus reducing to the case of the asymptotic distribution of the minimum of independent random variables)

We first show two auxiliary results:

Proposition 6.2. *Let T_N be a sequence of integer-valued non-negative random variables with corresponding generating functions $g_N(u) := \sum_{i=0}^{\infty} u^i \mathbf{P}(T_N > i)$ and c_N a sequence of positive numbers with $c_N \rightarrow 0$. Then $c_N T_N$ converges in distribution to a random variable T with $\mathbf{P}(T > t) = G(t)$ iff for each $p > 0$:*

$$c_N g_N(e^{-pc_N}) \rightarrow \int_0^{\infty} e^{-py} G(y) dy$$

Proof. Let f_N denote the probability generating function of T_N , so that $g_N(s) = \frac{1-f_N(s)}{1-s}$, and let $\ell_T(p) := \mathbf{E}(e^{-pT})$ denote the Laplace transform of T .

By the continuity theorem for Laplace transforms $T_N \rightarrow T$ in distribution iff $\ell_{T_N}(p) \rightarrow \ell_T(p)$ for each $p > 0$. " \Rightarrow ": let $c_N T_N \rightarrow T$ in distribution. Then $\ell_{c_N T_N}(p) = f_N(e^{-pc_N}) \rightarrow \ell_T(p)$ for each $p \geq 0$. Hence for $p > 0$

$$c_N g(e^{-pc_N}) = \frac{(1 - f_N(e^{-pc_N})) c_N}{(1 - e^{-pc_N})} \rightarrow \frac{1 - \ell_T(p)}{p} = \int_0^{\infty} e^{-py} G(y) dy$$

" \Leftarrow ": let for each $p > 0$

$$c_N g(e^{-pc_N}) = \frac{(1 - f_N(e^{-pc_N})) c_N}{(1 - e^{-pc_N})} \longrightarrow \frac{1 - \ell_T(p)}{p}$$

Then for each $p > 0$

$$1 - f(e^{-pc_N}) = c_N g(e^{-pc_N}) \frac{(1 - e^{-pc_N})}{c_N} \longrightarrow \frac{1 - \ell_T(p)}{p} p = 1 - \ell_T(p)$$

□

We have for $|u| < 1$:

$$g_{r,N}^{(1)}(u) =: \sum_{k=0}^{\infty} u^k \mathbf{P}(K_r^{(1)}(N) > k) = (n+1) \int_0^{\infty} \left(1 + (u-1) \frac{y}{1+y}\right)^{-(n+2)} Q_N(uy) dy$$

and

$$g_{r,N}^{(2)}(u) := \sum_{k=0}^{\infty} u^k \mathbf{P}(K_r^{(2)}(N) > k) = n \int_0^{\infty} e^{-n(1-u)y} Q_N(1 - e^{-uy}) dy$$

Combining this with the foregoing proposition gives:

Proposition 6.3. *Let s_N be a sequence of positive numbers s.th $s_N \rightarrow \infty$, $\frac{s(N)}{n(N)} \rightarrow 0$, and let T be a nonnegative random variable. Then we have:*

- (1) *if $s_N T_r^{(1)}(N)$ converges in distribution to T then $\frac{s_N}{n(N)+1} K_r^{(1)}(N)$ converges in distribution to T .*
- (2) *if $s_N T_r^{(2)}(N)$ converges in distribution to T then $\frac{s(N)}{n(N)} K_r^{(2)}(N)$ converges in distribution to T .*

Proof. Let $0 \leq u < 1$ and for $t \geq 0$ let $G(t) := \mathbf{P}(T > t)$.

Let $c_N := \frac{s_N}{n+1}$ and let $u := e^{-pc_N}$. Then

$$c_N g_{r,N}^{(1)}(e^{-pc_N}) = \int_0^{\infty} \left(1 + (e^{-c_N p} - 1) \frac{y}{s_N + y}\right)^{n+2} Q_N(e^{-c_N p} y / s_N) dy$$

Since $s_N T_r^{(1)}(N) \rightarrow T$ in distribution and since $c_N \rightarrow 0$ also $e^{c_N p} s_N T_r^{(1)}(N) \rightarrow T$. Thus $Q_N(e^{-c_N p} y / s_N) \rightarrow G(y)$ at all continuity points y of G . Further

$$(1 + (e^{-pc_N} - 1) \frac{y}{s_N + y})^n \rightarrow e^{-py}.$$

Moreover, the convergence is dominated since each $Q_N \leq 1$ and

$$(n+2) \log(1 - (1 - e^{-c_N p}) \frac{y}{y + s_N}) \leq -(n+2)(1 - e^{-c_N p}) \frac{y}{s_N + y} \leq -(n+2) c_N p e^{-c_N p} \frac{y}{s_N + y}$$

and therefore we can find a constant $c > 0$ s.th. for $y \geq 1$

$$(n+2) \log(1 - (1 - e^{-c_N p}) \frac{y}{y + s_N}) \leq -cyp$$

The dominated convergence theorem and proposition 6.2. now give the assertion.

The proof for (2) is similar.

□

Now let us prove (2) and (3):

assume that for each i the limit $\lim \rho_i(N) = \rho_i$ exists, and that $s_r(N) \rightarrow \infty$. It is then a routine matter to show that for $s_N := s_r(N)$ the random variables $s_N T_r(N)$ converge to the given distributions, and the additional assertions for (3) are also easy to show. An application of Proposition 6.3 finishes the proof. \square

Again some remarks are in order:

- (1) thus there are essentially three different types of limiting distributions and one will expect that for large domains and codomains the description by one of the types applies. Roughly speaking type (1) describes “almost injective” functions ($n \ll m$), type (2) describes “normal” functions ($n \approx m$) and type (3) describes “very surjective” functions
- (2) in any case $n/(s_r)^{1/r}$ is the correct measure for the appearance of the first collisions. The form of the distribution is easy to understand: the preimages which are small compared to this measure add to the “Weibull” factor, while the “large” preimages give the other factors. For “normal” mappings all preimages will be small compared to $n/(s_r)^{1/r}$, and the limiting distribution the Weibull- r distribution.
- (3) for the limiting distributions of R_r a completely analogous assertion as in part (2) holds (as may be deduced from theorems given by Camarri [3] (case $r > 2$), Camarri & Pitman [4] (case $r = 2$)):
if $v_r := (\sum_{i=1}^m x_i^r) \rightarrow \infty$, $\tilde{m}_r := n^r/v_r \rightarrow \infty$ and for each i the limit $x_i/(\tilde{m}_r)^{1/r} = \theta_i$ exists, then

$$\mathbf{P}(R_r > (\tilde{m}_r)^{(r-1)/r} t) \rightarrow e^{-(1-\sum_i \theta_i)t^r/r!} \prod_i e^{-\theta_i t} q_r(\theta_i t) \quad \text{for } 0 \leq t < \infty$$

Of course, both limits (i.e. θ_i and ρ_i) can exist at the same time and need not necessarily be the same. The special case of this theorem for uniformly small cells (i.e. $\theta_1 = 0$) is (at least implicitly) known for a long time. (See [19], Theorem 1 in III, §3)

- (4) It can be shown that in case (3) R_r has the same limit as K_r .
- (5) since $\tilde{m}_r \leq \min\{m^{r-1}, n^{r-1}\}$ an analogon to Thm 6.1, (1) cannot exist for R_r .
- (6) in cases (2) and (3) there is thus asymptotically no difference between drawing with or without replacement. In case (3) there is also never a difference between repetitions and collisions.

7. SUPPLEMENTARY CONSIDERATIONS

7.1. Asymptotic of $n/(s_r)^{1/r}$. It is clear from the above that $n/(s_r)^{1/r}$ characterises the behaviour of the r -collision times. How is the value of s_r distributed over all (n, m) -mappings? We consider again a uniform multinomial configuration (X_1, \dots, X_m) with parameters n and $p_1 = \dots = p_m = \frac{1}{m}$ and let

$$S_r^{(n,m)} = \sum_{i=1}^m \binom{X_i}{r}$$

the random variable “no. of r -collisions”.

Proposition 7.1. *If $n, m \rightarrow \infty$ s.th. $\frac{m^{r-1}}{n^r} \rightarrow 0$ then*

$$\frac{m^{r-1}}{n^r} S_r^{n,m} \rightarrow \frac{1}{r!} \text{ in distribution}$$

Proof. Calculations show that

$$(7.1) \quad \mathbf{E}(S_r^{(n,m)}) = \frac{1}{m^{r-1}} \binom{n}{r}$$

$$\text{Var}((S_r^{(n,m)})) = \left(\sum_{i=0}^{r-2} \binom{r}{i} \binom{n-r}{i} \frac{1}{m^i} + \left[\binom{n-r+1}{r} - \binom{n}{r} \right] \frac{1}{m^{r-1}} \right) \mathbf{E}(S_r^{(n,m)})$$

It is now easy to see that $\mathbf{E}(\frac{m^{r-1}}{n^r} S_r^{(n,m)}) \rightarrow \frac{1}{r!}$ and $\text{Var}((\frac{m^{r-1}}{n^r} S_r^{(n,m)})) \rightarrow 0$ \square

Thus if n is large compared to $m^{(r-1)/r}$ the effort for r -collision search will practically for every (n, m) function be of order $m^{(r-1)/r}$.

7.1.1. Balance measures. For uniform random mappings each colour i will appear with the same probability. The idea to measure the distance of a configuration from uniformity by a “balance measure” is near at hand. The classical statistic in this respect is the test-statistic of the χ^2 test, which in the case of a (n, m) uniform random mapping is:

$$T := \frac{m}{n} \sum_{i=1}^m (X_i - \frac{n}{m})^2 = \left(\frac{m}{n} \sum_{i=1}^m X_i^2 \right) - n$$

We know from the above that $n^2/S_2^{(n,m)}$ (or variants thereof) measures the performance of 2-collisions attacks. We have

$$T = m - n + \frac{2m}{n} S_2^{(n,m)}$$

Bellare and Kohno suggest to use

$$\mu_2 := -\log_m \left(\sum_{i=1}^m X_i^2 / n^2 \right)$$

to quantify resistance against a generic collision attack. This balance measure is related to 2-repetitions rather than to 2-collisions (this was earlier remarked by Wiener [30] and by Ramanna and Sarkar [23]). Clearly μ_2 is a simple variant of the χ^2 statistic T :

$$\mu_2 = 1 - \log_m(1 + T/n)$$

It is well known that $\mathbf{E}(T) = m-1$, $\text{Var}(T) = (1-1/n)(2m-2)$. Thus if $m, n \rightarrow \infty$ s.th. $m/n^2 \rightarrow 0$ then $\text{Var}(T/n) \rightarrow 0$ and $\mu_2 \approx 1 - \log_m(1 + \frac{m-1}{n})$. E.g for $n = am$ and large m this measure will have the value $\mu_2 = 1 - \log(1+1/a)/\log(m)$ for practically every (n, m) -function.

Ramanna and Sarkar suggest to use

$$\Lambda_r := -\frac{1}{r-1} \log_m \left(\frac{r! S_r^{(n,m)}}{n^r} \right)$$

to quantify resistance against a generic r -collision attack.

By Proposition 7.1, if $m, n \rightarrow \infty$ s.th. $m^{r-1}/n^r \rightarrow 0$ then $\text{Var}(r!m^{r-1}S_r^{(n,m)}/n^r) \rightarrow 0$. Thus if m^{r-1}/n^r is small this measure will have the value $\Lambda_r \approx 1 + \log_m(\frac{n^r}{(n)_r})$ for practically every (n, m) function.

From a probabilistic view these measures fail to uncover irregularities in a uniform random function: their scaling is too coarse. They only detect extreme deviations from uniform random behaviour.

7.2. On the difference between drawing with/without replacement.

7.2.1. Probability for true collisions. In this subsection we only consider drawing with replacement and write K_r for $K_r^{(2)}$. Here it is of interest to know the probability $\mathbf{P}(K_r = \min\{K_r, R_r\})$ that the first r -hit is caused by a true multi-collision. Let $E_{i,r}$ the event: i is the first colour which is drawn r -times (i.e. $E_{i,r} = \{X_{\min\{K_r, R_r\}} = i\}$). It is easy to show that

$$\mathbf{P}(K_r = R_r | E_{i,r}) = \frac{(x_i)_r}{x_i^r}$$

If $\ell := \min\{x_i | x_i \geq r\}$ and $M := \max\{x_i\}$ we therefore have

$$\frac{(\ell)_r}{\ell^r} \leq \mathbf{P}(K_r = R_r) \leq \frac{(M)_r}{M^r}$$

For $r = 2$ we can be more precise:

Theorem 7.2. *Let $b := |\{i : x_i > 0\}|$ the number of occupied images. Then the following inequalities hold*

$$\frac{n}{\sum_{i=1}^m x_i^2} \leq \mathbf{P}(R_2 < K_2) \leq \frac{b}{n}$$

Equality (on both sides) holds iff all positive x_i are equal.

Proof. (Sketch) Using generating functions one can derive that

$$\mathbf{P}(K_r = R_r) = \sum_{i=1}^m r \binom{x_i}{r} \int_0^\infty t^{r-1} e^{-nt} \prod_{j \neq i} q_r(x_j t) dt$$

Using the fact that $\sum x_i^2 t e^{-nt} \prod_{j \neq i} q_2(x_j t) = -(\prod_{i=1}^m F_2(x_i t))'$ where $F_2(t) = q_2(t)e^{-t}$ then

$$\mathbf{P}(R_2 < K_2) = \sum_{i=1}^m x_i \int_0^\infty t e^{-nt} \prod_{i \neq j} q_2(x_i t) dt$$

Let $p_i := \frac{x_i}{n}$ and $q := \sum_{i=1}^m p_i^2$ and rewrite the equality above as

$$\begin{aligned} n \mathbf{P}(R_2 < K_2) &= \int_0^\infty \left(\sum_{i=1}^l \frac{p_i s}{1+p_i s} \right) e^{-s} \prod_{i=1}^l (1+p_i s) ds \\ &= \int_0^\infty \left(\sum_{i=1}^l \frac{p_i s}{1+p_i s} \right) \exp(-s + \int_0^s \sum_{i=1}^l \frac{p_i}{1+p_i t} dt) ds \end{aligned}$$

(1) By Jensen's inequality $\sum_{i=1}^l \frac{p_i}{1+p_i s} \geq \frac{1}{1+qs}$, and therefore:

$$\begin{aligned} n \mathbf{P}(R_2 < K_2) &= \int_0^\infty \left(\sum_{i=1}^m \frac{p_i s}{1+p_i s} \right) \exp(-s + \int_0^s \frac{p_i}{1+p_i t} dt) ds \\ &\geq \int_0^\infty \frac{s}{1+qs} \exp(-s + \int_0^s \frac{1}{1+qt} dt) ds \\ &= \int_0^\infty \frac{s}{1+qs} e^{-s} (1+qs)^{\frac{1}{q}} ds \\ &= \frac{1}{q} \end{aligned}$$

(2) Another application of Jensen's inequality gives: $\sum_{i=1}^m \frac{p_i s}{1+p_i s} \leq \frac{s}{1+\frac{s}{b}}$. A similar computation then shows

$$n \mathbf{P}(R_2 < K_2) \leq b$$

□

7.2.2. Difference of expectations. Next we look at the order of magnitude of the difference of the collision times. We already saw that it is always preferable to use sampling without replacement, and that there is asymptotically no difference (on the $n/s_r^{1/r}$ scale) when both n and s_r tend to infinity. Here we quantify the difference more precisely.

Theorem 7.3. *There is a constant C_r (depending only on r) s.th.*

$$\mathbf{E}(K_r^{(2)}) - \mathbf{E}(K_r^{(1)}) < C_r n / (s_r)^{2/r}$$

Proof. (Sketch) We have

$$0 < \mathbf{E}(K_r^{(2)}) - \mathbf{E}(K_r^{(1)}) < n \int_0^\infty (1 - e^{-t}) \prod_{i=1}^m G_r(x_i, 1 - e^{-t}) dt =: n I$$

By lemma 9.4 from the appendix $\prod_{i=1}^m G_r(x_i, 1 - e^{-t}) \leq (e^{-td/s_r} q_r(dt/s_r))^{rs_r^{r+1}/d^r}$ where $d = \sum_{i=1}^m x_i \binom{x_i}{r}$ leading after simple steps to

$$I \leq \frac{s_r^2}{d^2} \int_0^\infty t (e^{-t} q_r(t))^{rs_r^{r+1}/d^r} dt$$

Using $rs_r^{r+1}/d^r \geq 1/r^{r-1}$ and observing that $c \mapsto c^{2/r} \int_0^\infty t (q_r(t) e^{-t})^c dt$ is decreasing finally shows that the assertion is true for

$$C_r = (1/r)^{2/r} \int_0^\infty t (e^{-t} q_r(t))^{1/r^{r-1}} dt$$

□

Thus the difference of expectations is $O(\frac{n}{(s_r)^{2/r}})$ (it is not hard to show that it is even $\Theta(\frac{n}{(s_r)^{2/r}})$ in Knuth's sense). This gives an independent proof for the fact that $\frac{s_r^{1/r}}{n} (K_r^{(2)} - K_r^{(1)}) \rightarrow 0$ if $s_r \rightarrow \infty$.

7.3. Cyclic points/ ρ -length for random fixed-indegree mappings.

The distribution of $K_2^{(1)}$ is closely related to two graph-theoretic distributions of random mappings. Let $\mathcal{D} = \{1, \dots, n\}$ and $f : \mathcal{D} \rightarrow \mathcal{D}$ an arbitrary function. The functional digraph G_f of f is the graph with vertices $\{1, \dots, n\}$ and directed edges $\{(1, f(1)), \dots, (n, f(n))\}$.

G_f consists of a number of connected components, each of which contains a unique cycle. In this way graph-theoretic terms can be applied to f , e.g. the cyclic points of f are the cyclic points in G_f etc. The indegree x_i of vertex i in G_f is $x_i = |f^{-1}(\{i\})|$.

Let in the sequel $c := (x_1, \dots, x_n)$ be a fixed indegree sequence (“configuration”), and let

$$\mathcal{F}_c := \{f : \mathcal{D} \rightarrow \mathcal{D} : |f^{-1}(\{i\})| = x_i \text{ for all } i\}$$

the set of mappings which share the same configuration. Let $Z(f)$ be the r.v. “number of cyclic points of f ” on \mathcal{F}_c , let $\rho(x, f)$ the r.v. on $\mathcal{D} \times \mathcal{F}_c$ “ ρ -length of x under f ”, let K be the r.v. “waiting time for the first collision” when drawing without replacement from an urn with configuration c (i.e. $K = K_2^{(1)}$, which was considered above). The following theorem holds:

Theorem 7.4. *Let $k \in \{0, \dots, n\}$.*

(a) *For the uniform distribution on \mathcal{F}_c*

$$\mathbf{P}(Z > k) = \mathbf{P}(K > k + 1)$$

(b) *For the uniform distribution on $\mathcal{D} \times \mathcal{F}_c$*

$$\mathbf{P}(\rho > k) = \frac{n - k}{n} \mathbf{P}(K > k)$$

Proof. We use variants of Prüfer-coding.

(a)(Foata-Fuchs) Each mapping from \mathcal{F}_c with leaves $y_1 < \dots < y_k$ can uniquely be encoded as a list of words (where word := list without repeated element) $w_0 \dots w_k$, where w_0 consists of the cycles of f (each coded as a word, starting with the largest element, and listing the remaining elements “against” the mapping direction, and these subwords concatenated in the ordering of their first elements), and the next word w_i is the “path” from l_i to its root x_i in $w_0 \dots w_{i-1}$, without y_i , but including its root x_i in $w_0 \dots w_{i-1}$, and listed against the mapping arrow, starting from x_i .

This coding gives a bijection between the set of mappings from \mathcal{F}_c with r cyclic points and the set of sequences with configuration c and first repeated value at $r + 1$.

(b) Each of the $n \binom{n}{x_1, \dots, x_n}$ possible choices of x, f (x starting point, $f \in \mathcal{F}_c$ mapping) can be encoded as a sequence of length $(n + 1)$:

$$(x = f^0(x), f(x), \dots, f^r(x), f(y_1), \dots, f(y_{N-r}))$$

where r is the smallest iterate where a previous element of the list is repeated, and $y_1 < \dots < y_{N-r}$ are the remaining elements (clearly x and f can be reconstructed from this list).

Thus there is a bijection between

(1) sequences of length $n + 1$, where the first element (no. 0) is drawn from

$\{1, \dots, n\}$, and the remaining elements are drawn without replacement from an urn with configuration c , with first repeated value at “time” $r + 1$, and
 (2) pairs (x, f) where x has rho-length r under f .
 Under this bijection, $\rho(x, f) > k$ iff $x_0 \notin \{x_1, \dots, x_k\}$ and x_1, \dots, x_k are pairwise distinct.

□

In an equivalent form (a) and (b) were earlier shown by Hansen and Jaworski ([12]). The asymptotic behaviour of Z resp. ρ can now directly be read off from Theorem 6.1, which generalises the corresponding results for Z and ρ in [1].

7.4. Application to generic collision search in hash functions.

“Real” hash functions H have (in principle) an infinite domain, and a finite range \mathcal{R} of cardinality $|\mathcal{R}| = m = 2^\ell$. However, restricted to an arbitrary finite input set they are concrete mappings with finite domain and range, and the theory given here applies.

If the attacker has no a priori knowledge about H and is given only “black box” access to H , the best he can do is to try to find collisions using “drawing without replacement”, i.e. hashing randomly chosen (non-repeating) input strings. In practice he has to restrict the possible input strings to a finite set \mathcal{D} of cardinality n (e.g. all input strings up to a certain maximal bitlength) and $h := H|_{\mathcal{D}}$ is a fixed (n, m) function. How many strings does he have to hash to find a collision? We know that $n/\sqrt{s_2}$ measures the effort for collision search. If n is large compared to \sqrt{m} the effort will be of order \sqrt{m} for practically every (n, m) function (see 7.1 and theorem 6.1, (2)). If n is of order \sqrt{m} in general at most a few collisions will exist. If they exist the trial of order \sqrt{m} is needed to find one (thm 6.1, (1)). Finally, if n is small compared to \sqrt{m} collisions are unlikely to exist (see the expected no. of collisions (7.1)).

Thus - unless the design of H is fundamentally flawed in the sense that the order of magnitude of $s_2(h)$ is larger than for a typical random (n, m) function - the typical effort will be of order \sqrt{m} . This is the basis for the folklore belief, that generic collision search (for a well designed hash function with codomain size m) needs an effort of \sqrt{m} . (In the same vein, a generic r -collision search (small, fixed r) needs an effort of $m^{(r-1)/r}$).

The plausibility of the \sqrt{m} -effort here rests on two assumptions:

- (1) the design of H ensures that the order of magnitude of $s_2(H|_{\mathcal{D}})$ is - for “canonical” (that is: easily specifiable, and not using specific properties of H) preimage sets \mathcal{D} of size n - comparable to that of the s_2 of a random (n, m) function
- (2) the attacker lacks the ability to specify a “favourable” preimage set

The first condition requires that H is well designed from a statistical point of view, and the second condition requires that H resists cryptanalysis.

The extent to which these conditions are fulfilled for a concrete hash function is debatable. If the attacker has a priori knowledge about H he may of course find specific attacks. Especially he may in this case be able to find a set \mathcal{A} of input strings s.th. a statistical collision attack on $h := H|_{\mathcal{A}}$ is “easy”. One of the main aims of hash function design is to make it “practically infeasible” for

an attacker to determine such input sets. (Although it is theoretically clear that such “favourable” input sets exist.)

REFERENCES

1. Arney, J. and Bender, E.A., *Random mappings with constraints on coalescence and the number of origins*, Pacific J. Math. 103 (1982), pp. 269–294.
2. Bellare, M. and Kohno, T., *Hash Function Balance and its Impact on Birthday attacks*. Advances in Cryptology - EUROCRYPT 2004, Lecture Notes in Computer Science 3027, pp. 401–419. Springer, Berlin, 2004, Full version available at <http://eprint.iacr.org/2003/065/>.
3. Camarri, M., *Asymptotics for k-fold repeats in the birthday problem with unequal probabilities*, Tech. report 524, Dept. Statistics, U. C. Berkley, Report, 1998.
4. Camarri, M. and Pitman, J., *Limit Distributions and Random Trees derived from the Birthday Problem with unequal Probabilities*, The Electronic Journal of Probability (2000).
5. Coppersmith, D., *Another Birthday Attack*. Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science 218, pp. 14–17. Springer, Berlin, 1985.
6. de Bruijn, N.G., *Asymptotic Methods in Analysis (3rd ed.)*. North Holland Publishing Co., Amsterdam, 1970, reprinted by Dover, 1981.
7. Diaconis, P. and Mosteller, F., *Methods for studying Coincidences*, Journal of the American Statistical Association 84 (1989), pp. 853–861.
8. Flajolet, P. and Gardy, D. and Thimonier, L., *Birthday Paradox, Coupon Collectors, Caching Algorithms and Self-organizing Search*, Discrete Applied Mathematics 39 (1992), pp. 207–229.
9. Flajolet, P. and Sedgewick, R., *Analytic Combinatorics*. Cambridge University Press, Cambridge (UK), 2009.
10. Girault, A. and Cohen, R. and Campana, M., *A Generalized Birthday Attack*. Advances in Cryptology - EUROCRYPT '88, Lecture Notes in Computer Science 330, pp. 129–157. Springer, Berlin, 1988.
11. Good, I.J., *Saddle-point Methods for the Multinomial Distribution*, Ann. Math. Stat. 28 (1957), pp. 861–881.
12. Hansen, J.C. and Jaworski, J., *Random mappings with exchangeable in-degrees*, Random Struct. Algorithms 33 (2008), pp. 105–126.
13. Holst, L., *On birthday, collectors', occupancy and other classical urn problems*, International Statistical Review 54 (1986), pp. 15–27.
14. Holst, L., *The General Birthday Problem*, Random Struct. Algorithms 6 (1995), pp. 201–208.
15. Johnson, N.L. and Kotz, S., *Application of Urn Models*. John Wiley and Sons, Inc., Chichester, 1977.
16. Joux, A., *Multicollisions in Iterated Hash Functions. Applications to Cascaded Constructions*. Advances in Cryptology - CRYPTO 2004, Lecture Notes in Computer Science 3152, pp. 306–316. Springer, Berlin, 2004.
17. Klamkin, M.S. and Newman, D.J., *Extensions of the Birthday Surprise*, Journal of Combinatorial Theory 3 (1967), pp. 279–282.
18. Knuth, D.E., *The Art of Computer Programming, vol. 1 (3rd. ed.)*. Addison-Wesley Publishing Company, Reading, Massachusetts, 1997.
19. Kolchin, V.F. and Sevast'yanov, B.A. and Chistyakov, V.P., *Random Allocations*. V.H. WINSTON & SONS, Washington, D.C., 1978.
20. Laccetti, G. and Schmid, G., *On a Probabilistic Approach to the Security Analysis of Cryptographic Hash Functions*, Cryptology ePrint Archive, Report no. 324, 2004. Available at <http://eprint.iacr.org/2004/324>.
21. Nandi, M. and Stinson, D.R., *Multicollision Attacks on Some Generalized Sequential Hash Functions*, Cryptology ePrint Archive, Report no. 055, 2006. Available at <http://eprint.iacr.org/2006/055>.

22. Preneel, B., *Analysis and Design of Cryptographic Hash Functions*, Ph.D. thesis, K.U. Leuven, Leuven, Belgium, 1993.
23. Ramanna, S.C. and Sarkar, P., *On Quantifying the Resistance of Concrete Hash Functions to Generic Multi-Collision Attacks*, Cryptology ePrint Archive, Report no. 525, 2009. Available at <http://eprint.iacr.org/2009/525>.
24. Schulte-Geers, E., *Problem 11353*, American Mathematical Monthly 115 (2008), p. 263.
25. Stinson, D.R., *Some Observations on the Theory of Cryptographic Hash Functions*, Cryptology ePrint Archive, Report no. 020, 2001. Available at <http://eprint.iacr.org/2001/020>.
26. Stong, R., *Solution to problem 11353*, American Mathematical Monthly 117 (2010), pp. 91–92.
27. Suzuki, K. and Tonien, D. and Kurosawa, K. and Toyota, K., *Birthday Paradox for Multicollisions*. Information Security and Cryptology - ICISC 2006, Lecture Notes in Computer Science 4296, pp. 29–40. Springer, Berlin, 2006.
28. von Mises, R., *Über Aufteilungs- und Besetzungswahrscheinlichkeiten*, Revue de la Faculté des Sciences de l' Université d'Istanbul 4 (1939), pp. 145–163. reprinted in [29].
29. ———, *Selected Papers of Richard von Mises, vol. 2*, pp. 313–334. American Mathematical Society, Providence, R.I., 1964.
30. Wiener, M.J., *Bounds on Birthday Attack Times*, Cryptology ePrint Archive, Report no. 318, 2005. Available at <http://eprint.iacr.org/2005/318>.

8. APPENDIX

In this appendix we collect some inequalities.

Lemma 8.1. *Let X be binomial distributed with parameters n and p . For $r < n$*

$$\mathbf{P}(X < r) \geq (1 - p^r)^{\binom{n}{r}}$$

Proof. Let $f(p) := \log(\mathbf{P}(X < r)) - \binom{n}{r} \log(1 - p^r)$ the log of the quotient lhs/rhs. We find

$$f'(p) = -r \binom{n}{r} \left(\frac{p^{r-1}(1-p)^{n-r}}{\mathbf{P}(X < r)} - \frac{p^{r-1}}{1-p^r} \right) = r \binom{n}{r} p^{r-1} \left(\frac{\mathbf{P}(X < r) - (1-p)^{n-r}(1-p^r)}{\mathbf{P}(X < r)(1-p^r)} \right)$$

The numerator of the rhs is of the form $\mathbf{P}(S_n \leq r-1) - \mathbf{P}(S_{n-r} = 0)\mathbf{P}(S_r < r-1)$ and is therefore nonnegative. Thus $f(p) \geq f(0) := 0$, i.e. the quotient is ≥ 1 . \square

Lemma 8.2. *For $s \geq 0$, $n > r$*

$$-\log G_r(n, 1 - e^{-s}) \leq \binom{n}{r} s^r$$

Proof. Let $f(s) := -\log(G_r(n, 1 - e^{-s})) - \binom{n}{r} s^r$. We find

$$f'(s) = r \binom{n}{r} \left(\frac{(e^s - 1)^{r-1}}{p_r(n, e^s - 1)} - s^{r-1} \right)$$

Clearly $p_r(n, e^s - 1) \geq p_r(r-1, e^s - 1) = e^{(r-1)s}$. Thus

$$f'(s) \leq (1 - e^{-s})^{r-1} - s^{r-1} \leq 0$$

Thus $f(s) \leq f(0) := 0$. \square

Lemma 8.3. *Let $F_r(s) := q_r(s)e^{-s}$. Then for $s > 0$*

$$-\log(F_r(s)) \leq \frac{s^r}{r!}$$

Proof. Similar as above. \square

Lemma 8.4. *Let $d := \sum_{i=1}^m x_i \binom{x_i}{r}$ and $s_r := \sum_{i=1}^m \binom{x_i}{r}$. Then for $t > 0$*

$$\prod_{i=1}^m G_r(x_i, 1 - e^{-t}) \leq \left(e^{-t} q_r\left(\frac{d}{s_r} t\right) \right)^{rs_r^{r+1}/d^r}$$

Proof. Let $f(t) := \sum_{i=1}^m \log(G_r(x_i, 1 - e^{-t}))$. We find

$$f'(t) = - \sum_{i=1}^m r \binom{x_i}{r} \frac{(e^t - 1)^{r-1}}{p_r(x_i, e^t - 1)} \leq - \sum_{i=1}^m r \binom{x_i}{r} \frac{t^{r-1}}{q_r(x_i t)}$$

Since $t \mapsto 1/q_r(t)$ is convex on \mathbf{R}_+ Jensen's inequality gives $\sum_{i=1}^m \binom{x_i}{r} \frac{1}{q_r(x_i t)} \geq \frac{s_r}{q_r(\frac{d}{s_r} t)}$ and so

$$f'(t) \leq - \frac{rs_r t^{r-1}}{q_r(\frac{d}{s_r} t)} = \frac{rs_r^{r+1}}{d^r} (\log F_r(\frac{d}{s_r} t))'$$

where F_r is as in lemma 8.3. Thus the log of the quotient lhs/rhs is decreasing in t . \square

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, GODESBERGER ALLEE 185–189,
53175 BONN, GERMANY

E-mail address: ernst.schulte-geers@bsi.bund.de